

---

# BGIN Block #10 Meeting Report

*- BGIN is a multi-stakeholder discussion body / distributed think tank.*

## Illicit Activity

---

**bg  
in**

**b**lockchain  
**g**overnance  
**i**nitiative  
**n**etwork

**The Global Network for Blockchain Stakeholders™**

© 2023 BGIN (Blockchain Governance Initiative Network) is registered as BN Association, a Japanese general association with its principal place of business at Shiba Building, 704, 4-7-6, Shiba, Minato-ku, Tokyo. All rights reserved.

The know-how described in this document was made available from contributions from various sources, including members of the BGIN and others. Although the BGIN has taken steps to help ensure that the know how is available for distribution, it takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the know how described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any independent effort to identify any such rights. BGIN and the contributors to this document make no (and hereby expressly disclaim any) warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this document, and the entire risk as to implementing this document is assumed by the implementer. The BGIN Intellectual Property Rights policy requires contributors to offer a patent promise not to assert certain patent claims against other contributors and against implementers. BGIN invites any interested party to bring to its attention any copyrights, patents, patent applications, or other proprietary rights that may cover technology that may be required to practice this document.

## Block#10 Day2\_13

Keynote Session Report: Illicit Activity

Date: Monday, March 4, 2024

Location: Tokyo

Duration: Approx. 90 minutes

## Summary

### Introduction and Perspectives on Illicit Activities

- The conversation focuses on illicit activities, where a discussant provides a basic definition related to jurisdictional laws. Other discussants expand on this by introducing a typology map, illustrating the various categories of illicit activities and money laundering processes involved in the crypto space.

### Diverse Views on Illicit Activities and Their Impact

- Discussants discuss the complexities of defining illicit activities and how these definitions vary across jurisdictions and industries. The role of blockchain analytics companies in categorizing and providing data on such activities is highlighted, emphasizing the importance of accuracy and timeliness in data attribution. A discussant shares her multifaceted experience and emphasizes the need for a clear understanding of what constitutes illicit activity in different contexts.

### Challenges Faced by Law Enforcement and Compliance Officers

- The discussion turns to the practical challenges faced by law enforcement and compliance officers in dealing with illicit activities, especially in the context of resource constraints and the vast array of potential crimes. The discussants acknowledge the crucial role of high-quality data and legal clarity in aiding these efforts. The importance of blockchain analytics tools in providing actionable insights is also discussed, with emphasis on their role in making illicit activities more visible and, therefore, harder to ignore.

### The Role of Blockchain Analytics and the Need for Common Standards

- Discussants explore the significant role of blockchain analytics companies in shaping the understanding and approach towards illicit activities within the crypto space. The

conversation touches upon the potential benefits of establishing common standards or taxonomies for categorizing illicit activities, which could facilitate better interoperability among different analytics tools and enhance the efficiency of compliance processes.

### Balancing Regulation with Innovation and Privacy Concerns

- The dialogue shifts to the balance between regulation, innovation, and privacy concerns, particularly in relation to tools like mixers that enhance privacy on the blockchain. The discussants discuss the regulatory perspective on such tools, acknowledging the challenges in distinguishing between legitimate privacy needs and potential misuse for illicit purposes. The need for ongoing dialogue between regulators, industry players, and analytics companies is emphasized to ensure that innovation is not stifled while maintaining robust measures against illicit activities.
- The discussants reflect on the key themes discussed, including the importance of high-quality data, the potential benefits of common standards in categorizing illicit activities, and the ongoing challenges in balancing privacy rights with regulatory requirements. They also reflect on an acknowledgment of the complex landscape of illicit activities in the crypto space and a call for continued collaboration among stakeholders to address these challenges effectively.

### Discussion on Mixers and Their Legal Implications

- The discussion opens with a debate about the legal implications of mixers in the context of sanctions. Discussants explore the challenges in classifying mixers due to their association with both legitimate privacy concerns and potential illicit activities. The conversation delves into the nuances of labeling and categorizing blockchain activities, emphasizing the responsibility of compliance officers to investigate alerts rather than making assumptions based on labels alone.

### The Role of Blockchain Analytics and the Importance of Accurate Data Labeling

- Discussants discuss the critical role of blockchain analytics companies in providing data that helps in identifying potentially illicit activities. The conversation highlights the importance of accurate data labeling and the distinction between data as a starting point for investigation versus a conclusive indicator of illicit activity. The discussion also touches on the potential for standardization in the industry to facilitate a more unified approach to identifying and addressing illicit activities.

### Challenges of Peer-to-Peer Transactions and Standardization Efforts

- A question from the audience about managing peer-to-peer transactions and the potential consequences of inadvertently receiving illicit crypto sparks a discussion on the practical

challenges individuals and platforms face. The conversation then shifts towards the efforts and challenges in creating standardized taxonomies and frameworks within the industry to address illicit activities more effectively. Discussants express varied opinions on the feasibility and potential impact of standardization, with some highlighting the importance of industry-led initiatives and others cautioning about the complexities and unintended consequences of such efforts.

#### Concluding Thoughts and Future Directions

- The session ends with an open invitation for further dialogue and collaboration within the industry to develop effective strategies and standards for combating illicit activities in the crypto ecosystem.

#### Transcript (anonymized) :

04:00:24

The session moves towards formal introductions, starting with an individual who introduces themselves and their role in a blockchain-focused group. They outline the group's focus areas beyond the basics of blockchain technology, setting the stage for discussions on the panel's central theme of illicit activities in the field.

04:01:34 - 04:02:55

Successive introductions highlight the diverse backgrounds of the panelists, ranging from blockchain data analytics to regulatory and policy advisory roles. Each panelist shares their professional journey, touching upon previous affiliations with governmental and private sectors, and their current engagements in blockchain analytics and regulatory frameworks.

04:03:00

The session includes a remote participant who delves into a detailed account of their multifaceted career. This encompasses roles from teaching to legal and investigative positions, emphasizing their expertise in financial crimes and compliance across various jurisdictions. The participant also mentions certifications in data protection and cryptocurrency tracing, underscoring their comprehensive skill set in addressing complex challenges in the field.

04:04:47

The conversation shifts to the diverse perspectives on illicit activities, inviting definitions and explanations from the participants to foster a comprehensive understanding of the topic.

04:05:06

The term 'illicit activities' is defined as actions not accepted under the jurisdiction's laws, with emphasis on the variability depending on the jurisdiction, illustrated with the example of gambling's legal status differing across regions.

04:06:07

Expanding on this, another viewpoint is presented on illicit activities in the financial context, categorizing them into revenue-generating crimes and the laundering of such proceeds through various means, including blockchains. A detailed exploration of crime typologies and the stages of money laundering within the cryptocurrency ecosystem is provided, highlighting the complexity and global nature of these illicit activities.

04:08:50

A reflection on the provided taxonomy of illicit activities acknowledges its complexity and sophistication, prompting a query about agreement or alternative views on the categorization.

04:09:03

In response, the nuanced nature of defining illicit activities is discussed, stressing the importance of understanding the purpose and context of identifying such activities. The conversation underscores the challenges faced by entities in the blockchain analytics space in navigating the global landscape of varying legal standards and the imperative of risk management in compliance efforts.

04:11:13

The challenge of delineating clear boundaries around acceptable and unacceptable exposures is acknowledged, emphasizing the feasibility of having 'fuzzy boundaries' as long as there's an understanding of primary concerns. The discussion suggests starting with universally recognized illicit activities, like child sex abuse material (CSAM), as a foundation for building a comprehensive approach, accepting the evolving nature of categorizing illicit activities without seeking a flawless solution immediately.

04:12:12

Acknowledging the holistic approach as valuable yet challenging, the dialogue moves towards pragmatic applications of the agreed taxonomy, particularly in law enforcement and risk management within the blockchain ecosystem, highlighting the need for a tailored approach based on jurisdictional laws and the operational scope of entities.

04:13:15

The conversation shifts to a user perspective, seeking agreement on the approach and its utility in practical scenarios, emphasizing the importance of identifying common denominators in criminal activities across different legal landscapes while respecting individual nation-states' laws.

04:14:28

Drawing on personal experience, the emphasis is placed on the pragmatic aspects of using analytics software in tracing crypto transactions for complex investigations, considering local laws and the necessity of a practical approach in managing global risk and compliance, especially in the decentralized and borderless nature of the cryptocurrency ecosystem.

04:15:43

The value of establishing a common standard for global operations is highlighted, alongside the appreciation for the taxonomy chart as a useful tool in understanding and managing illicit activities within the crypto space.

04:16:08

The conversation turns to the role of global companies in defining a common denominator for illicit activities, pondering whether industry consensus or governmental agreement should prevail, and speculating on the potential role of international bodies in promoting such standards.

04:17:18

Focusing on the practical application of the taxonomy in preventing money laundering through legitimate crypto services, the discussion emphasizes the critical role of exchanges and payment gateways as gatekeepers in the ecosystem, and the need for implementable standards that address the complexities of tracking and blocking illicit transactions.

04:18:27

The inquiry here revolves around the application and clarity of guidelines within the current regulatory frameworks, especially considering the industry's nascent stage. The speaker is pondering whether it's practical to compartmentalize regulations or adhere to universal standards that cover broad categories like sanctions and child abuse material. The emphasis is on the simplicity and feasibility for compliance officers who often rely on a risk-based approach due to the lack of clear jurisdictional guidance and the complex nature of exposure assessments in the industry.

04:19:13

The conversation continues with a focus on the challenges faced by compliance officers, who must navigate an industry filled with uncertainties and ambiguities, particularly regarding

jurisdictional directives and the extent of indirect exposures. The reliance on a risk-based approach by risk officers is highlighted, given the industry's complex nature.

04:19:35

Here, the discussion points to the lack of definitive guidance from regulators on how far compliance officers should go in their due diligence processes, especially when it involves tracing activities or transactions multiple steps removed from the initial point. The importance of creating practical and effective regulatory frameworks is underscored, taking into account the industry's maturity and the practical challenges faced by those who will implement these frameworks.

04:20:13

A different perspective is introduced, acknowledging general agreement with previous points but emphasizing the unique role of blockchain analytics companies in creating taxonomies that shape regulatory and compliance strategies. The nuances in categorizing fraudulent activities and their significance in compliance and law enforcement are discussed, illustrating the complexities involved in accurately identifying and addressing different types of fraudulent activities within the regulatory frameworks.

04:20:47

The conversation delves into the intricacies of financial crime categorization and its implications for compliance strategies within financial institutions. The differentiation between various types of financial crimes and their relative importance to compliance officers is highlighted, with a particular focus on the paramount importance of sanctions compliance due to the severe consequences of non-compliance.

04:21:04

The discussion expands on the prioritization challenges faced by compliance officers, particularly in distinguishing between urgent and less urgent matters within the broad spectrum of financial crimes. The reality of resource constraints and the necessity of triage in compliance activities are emphasized, illustrating the practical considerations that shape the day-to-day decisions of compliance professionals in the financial industry.

04:21:48

The speaker discusses the practical realities of compliance work in the financial sector, particularly within the context of cryptocurrency transactions. The challenges of maintaining visibility and conducting effective compliance in a sector characterized by anonymity and a lack of traditional banking safeguards like KYC (Know Your Customer) protocols are highlighted, underscoring the complex landscape in which compliance officers operate.

04:22:38

Discussing the role of blockchain analytics companies, it's highlighted that these organizations provide unprecedented visibility into the flow of illicit funds within the crypto space. This visibility is contrasted with traditional banking practices, where assessments of suspicious activity are often more rudimentary. The significance of the analytics companies' role in determining relevant data for financial institutions is emphasized, pointing out the critical nature of accurate data classification and its impact on financial compliance and crime prevention.

04:24:22

A narrative is shared about an encounter with a person during a buffet lunch, where a conversation about personal values and dietary choices leads to a broader reflection on prioritization and value alignment. The story serves as an analogy for the importance of prioritizing critical issues like child abuse and human trafficking in financial compliance, suggesting that these issues should perhaps be given greater emphasis in the context of financial crime prevention and compliance scoring systems, similar to how cybersecurity threats are prioritized.

04:26:08

Reflecting on the prioritization of compliance issues, it's noted that what is deemed most critical can vary significantly depending on an organization's specific risk profile. Some may place equal emphasis on combating child sexual abuse material (CSAM) and adhering to sanctions, with the understanding that sanctions carry a strict liability. The importance of not overgeneralizing priorities across different entities is highlighted.

04:27:00

Drawing from experiences as a prosecutor and interactions with blockchain analytics firms, the importance of data quality in the attribution and classification of transactions is emphasized. Recognizing the strengths and weaknesses of different analytics companies, the conversation acknowledges their crucial role in the accuracy and effectiveness of compliance efforts within the industry.

04:28:04

A clarification is sought regarding a previous comment, suggesting that reevaluating underlying assumptions might lead to a reassessment of values, particularly in the context of behavioral and financial decision-making.

04:28:35

Adding to the discussion, the impact of having access to specific data, akin to knowing the caloric content of food, on decision-making processes is discussed. This analogy extends to the realm of cryptocurrency and crime, highlighting how increased transparency and data can transform the approach to crime prevention and compliance, potentially altering behaviors and priorities in the process.

04:29:26

Highlighting the stark visibility that blockchain analytics provides into illicit financial activities, it's pointed out that this transparency challenges law enforcement and regulatory bodies to confront issues like money laundering and terrorist financing head-on. The analogy continues with the emphasis on the ease of identifying illicit activities through blockchain analytics, contrasting sharply with traditional financial systems where such activities were more easily obscured.

04:31:31

Discussing the crucial role of those who interpret and act upon the data provided by blockchain analytics, the importance of skilled compliance officers is underscored. It's mentioned that regulatory bodies, like the UK's Financial Conduct Authority, expect entities to not only possess analytical tools but also to have personnel proficient in applying these tools to the specific risks faced by their organization. This highlights the idea that while analytics tools provide critical insights, the ultimate responsibility for action lies with the individuals and entities using these tools.

04:33:00

Addressing the question about what is needed to enhance the utility of data platforms for users, the discussion touches on the importance of high-quality data, legal clarity, and more effective use of tools. Regulation is identified as a potential driver to encourage widespread adoption of these platforms, improving both the timeliness of information sharing and the collective benefit to the ecosystem.

04:34:39

The conversation further explores the value of improved information exchange, particularly with law enforcement, to enrich data platforms and make actionable intelligence more readily available. This would enable users to address issues more proactively, reducing the ability to ignore problematic data.

04:36:03

The evolving nature of the categories tracked by blockchain analytics tools is emphasized, acknowledging the need for continuous adaptation to emerging concerns in the crypto space. Feedback from the ecosystem is deemed crucial for guiding these adaptations.

04:36:54

Legal clarity is highlighted as a significant area where support is needed. The ambiguity surrounding certain activities, such as the exploitation of smart contract vulnerabilities, poses challenges in categorizing actions as illicit. The development of legal precedents and clearer legal frameworks is anticipated to provide more definitive guidance for classifying and responding to such activities within the analytics platforms.

04:37:44

Highlighting the disparities in resources among different levels of law enforcement, it's argued that the assumption that knowledge of illicit activities compels action overlooks the practical limitations faced by local law enforcement. The challenges include a lack of access to advanced investigative tools, jurisdictional constraints, and the overwhelming volume of cases, particularly related to scams and money laundering, which necessitates a triage approach due to limited resources.

04:39:52

The discussion then shifts to the assumption that startups, especially in the crypto space, have the means to afford advanced blockchain analytics tools. Given the financial constraints typical of startups, the expectation from regulators for these entities to have not just one, but multiple tools for cross-referencing, is highlighted as a significant challenge. This underscores a gap between regulatory expectations and the practical financial capabilities of emerging companies.

04:41:40

Responding to these concerns, the importance of data in helping both law enforcement and regulatory bodies prioritize their limited resources is emphasized. While acknowledging the constraints, it's suggested that analytics data can guide focused efforts on the most critical areas. From a regulatory perspective, the approach does not mandate specific tools but encourages measures appropriate to the size and scale of the business, aiming for practical and adaptable compliance solutions.

04:42:16

Addressing the challenges faced by startups in the financial sector, it's noted that regulatory expectations can set a high barrier to entry. Startups may be able to use open source tools for due diligence, depending on their business size and target market. The conversation acknowledges the learning curve and mutual unfamiliarity between the crypto industry and regulators when

regulatory frameworks were first introduced, highlighting the unique difficulties startups face in this sector.

04:43:33

Clarifying a previous point, the emphasis is placed on the challenges at the federal level, particularly in addressing issues like terrorist financing. The discussion points to instances where significant financial crimes were overlooked due to a lack of political will, despite having the necessary resources to address them. The contrast with the heightened visibility and urgency attributed to similar issues within the crypto space is highlighted, suggesting a discrepancy in response based on the visibility of the issue rather than its inherent severity or urgency. The clarification aims to distinguish between resource constraints at local levels of law enforcement and broader systemic issues, including political motivations, that affect the prioritization and response to financial crimes.

04:45:24

Discussing the various challenges faced by the industry, including political will, resource constraints in the startup world and public sector, lack of expertise in deploying and using tools, and unclear government regulations, the conversation shifts to the idea of establishing common standards. Drawing an analogy from the field of cryptography, where the industry is moving towards agreed-upon standards for cryptographic keys, the possibility of creating similar standards for categorizing and prioritizing financial crimes in the crypto space is proposed.

04:47:16

Reflecting on the nature of crimes associated with cryptocurrency, it's noted that many of these are not new but are traditional crimes facilitated in a new medium. The continuity of criminal activities like sanctions evasion, terrorist financing, and scams, whether through traditional fiat systems or cryptocurrency, is emphasized. The discussion suggests that existing frameworks in the traditional financial space could serve as a reference for standardizing approaches in the crypto sector, without the need to invent new categories specifically for cryptocurrency.

04:49:32

Human trafficking and terrorist financing are persistent issues, and despite frequent news coverage, there's a risk of law enforcement becoming desensitized to these problems. Developing a standard taxonomy for financial crimes, while taking traditional finance as a reference point, is essential. However, it's important to acknowledge that law enforcement agencies may prioritize different aspects based on current pressures and "crimes of the moment." For instance, a few years back, Initial Coin Offerings (ICOs) drew significant attention due to the potential for financial loss. Currently, scams represent a major concern, not necessarily related to cryptocurrencies but affecting various financial systems. These scams involve complex

processes, like money mules and bank transfers, leading to cryptocurrencies in some cases. This doesn't diminish the significance of cryptocurrencies in the broader landscape of financial crime. Establishing a clear and aligned taxonomy could facilitate better understanding and management of these issues.

04:50:17

The focus on scams, which are now widespread and can involve both digital and traditional currencies, highlights the evolving nature of financial crimes. Law enforcement's attention to scams, especially in places like Singapore where they are frequently reported, does not mean that cryptocurrency-related issues are overlooked. Instead, these are part of a larger financial crime ecosystem that needs to be addressed comprehensively. Achieving alignment in the classification and understanding of these crimes could aid in more effective management and prevention efforts.

04:51:02

The challenge extends beyond merely categorizing financial crimes; it involves making these categories specific enough for automation and simplification for all stakeholders. This requires precise definitions, terminologies, and data formats, not only for legal documentation but also for integration into software used by exchanges and startups. This precision is necessary for seamless connectivity and efficient operation within the financial system.

04:51:34

Leading analytics firms have already established clear definitions for various financial crimes, such as ransomware and malware, within their applications. However, there's a noticeable disparity in the number of categories recognized by different organizations, which could range from 20 to 50. This variation points to the need for a more unified approach that can offer a holistic view of financial crimes, facilitating better understanding and more effective countermeasures across the board.

04:52:09

The discussion centers around the possibility of establishing a standard across the industry to ensure uniformity regardless of the specific products being used. This standard would help in creating a consistent approach to categorizing and addressing various aspects of financial crimes across different platforms.

04:52:22

The idea of a common inventory specification, similar to practices in other industries, is proposed. This would allow for a unified database system where data from various sources can be integrated and utilized efficiently. The goal is to achieve a level of interoperability where,

despite the diversity of tools and data origins, there can be seamless movement and application of information.

04:52:44

It's argued that the disparity in tools and categorizations may not be as significant an issue as perceived, considering the current trend towards API integration. Law enforcement agencies, for example, are already combining multiple tools through APIs to enhance their investigative capabilities. This approach allows for a more comprehensive analysis, enabling agencies to draw from various sources without being confined to the limitations of any single tool.

04:53:26

The discussion shifts towards the impact of a common taxonomy on compliance officers (CCOs) within financial institutions. The varying categorizations between tools can create inefficiencies and complicate risk assessment processes. For compliance purposes, a unified taxonomy could greatly reduce such frictions, making it easier for financial institutions to set and manage their risk tolerance effectively.

04:54:10

The notion is introduced that, for law enforcement, the varied categorizations serve more as initial leads rather than definitive categorizations of criminal activity. Given that criminals often engage in multiple types of crimes, the exact categorization might be less critical in the context of law enforcement investigations.

04:54:18

The conversation concludes with a focus on the importance of a common taxonomy not just for data integration, but also for the entire lifecycle of compliance and remediation processes. For end users, particularly in financial institutions and exchanges, the ability to integrate multiple tools effectively and act upon the insights gained is crucial. This includes not just the identification and categorization of activities but also the subsequent actions such as remediation, issuing recommendations, and automating responses to potential threats.

04:54:56

The conversation emphasizes the importance of interoperability among APIs in the financial sector, highlighting the benefits of having a common data language for multiple API analyses. This interoperability is deemed particularly beneficial for financial institutions, where the reliance on multiple data sources is common. The future likely entails extensive integration of diverse datasets, making a unified approach to data categorization increasingly valuable.

04:55:43

The idea of a consistent taxonomy across APIs is further supported, suggesting that such uniformity would enhance the overall system for all users. This consistency is seen as a way to streamline processes and reduce potential discrepancies when analyzing data from multiple sources.

04:55:55

Technical challenges are acknowledged, such as discrepancies in categorization across different systems, which can lead to confusion and inefficiency. For instance, if three systems analyze the same data but yield different categorizations, it complicates the decision-making process for compliance officers, who then must navigate these inconsistencies.

04:56:41

The difficulty faced by compliance officers in resolving categorization discrepancies is highlighted. The process of reconciling different categorizations from multiple systems can be cumbersome, involving significant communication and justification efforts with each system provider.

04:57:41

Drawing parallels with the evolution of cybersecurity standards, the conversation reflects on the importance of educating the industry and establishing recognized standards. Similar to how cybersecurity standards evolved to provide general guidelines without prescribing specific tools, a common taxonomy in financial data analysis could offer a framework for categorization without dictating specific solutions.

04:58:32

The discussion suggests that the financial industry could benefit from agreeing on a set of standard categories for financial crimes, similar to how cybersecurity standards have been established. This would not mandate specific protective measures but would define common categories, such as scams, to ensure industry-wide alignment.

04:59:17

The practical application of a unified taxonomy is discussed, with an emphasis on the ease of compliance and auditing processes it could facilitate. By aligning on definitions and categories, industry players can more efficiently demonstrate their protective measures against various financial crimes during audits, enhancing clarity and compliance.

04:59:43

The conversation acknowledges the value of standards in promoting adoption and potentially becoming a requirement for regulatory compliance. This approach is recognized as a feasible way forward in achieving uniformity across the industry.

05:00:01

A counterpoint is raised regarding the potential conflict between a unified definition of financial crimes, such as scams, and the sovereign rights of individual nations to define criminal activities according to their local laws. The importance of balancing the efficiency gained from automation and standardization with the need to respect local legal frameworks is highlighted.

05:00:43

The discussion delves into the complexities of reconciling standardized definitions of financial crimes with national legal systems, particularly focusing on the nuances of data protection and privacy. The concern is that a universal approach to defining and categorizing financial crimes might inadvertently infringe upon individual rights and local legal definitions.

05:01:49

An example is given concerning privacy tools on the blockchain, where the default assumption of criminal intent associated with privacy-enhancing technologies is questioned. The debate underscores the potential consequences of generalizing definitions in an attempt to automate compliance processes, which could lead to misinterpretations regarding the use of privacy tools.

05:02:55

The discussion extends to the comparison of privacy expectations between traditional banking and blockchain transactions, emphasizing the need for a careful approach to automation and classification to avoid unintended consequences that might compromise individual privacy.

05:03:27

The dialogue acknowledges the complex regulatory landscape surrounding privacy tools, particularly mixers, and the ongoing debate about balancing privacy rights with the prevention of illicit activities.

05:03:35

The regulatory challenges associated with privacy-enhancing technologies like mixers are discussed, highlighting the high-profile concerns about their association with illicit activities. The conversation reflects on the industry's efforts to address these concerns while maintaining the legitimate right to privacy for users.

05:04:20

A mention of a recent congressional hearing explores the delicate balance between safeguarding privacy and preventing illicit use of privacy-enhancing technologies, illustrating the broader challenges faced by the industry in navigating new innovations and market dynamics.

05:05:00

The legal obligations of platforms to reflect sanctions on certain mixers are discussed, with a focus on managing the tension between regulatory compliance and the potential overgeneralization of criminal intent among mixer users.

05:05:24

The process of investigating alerts from transactions involving mixers is described, emphasizing the importance of not jumping to conclusions and conducting thorough investigations based on customer risk profiles and due diligence information.

05:06:14

The challenges faced by exchanges and other crypto entities in developing risk-based approaches are highlighted, including the reliance on default settings provided by analytics tools and the potential for unintended consequences from conservative, risk-averse actions.

05:07:32

The responsibility of compliance departments in interpreting and acting on the classifications provided by blockchain analytics tools is underscored, cautioning against over-reliance on these classifications without adequate investigation and due diligence.

(The recording accidentally stopped, and the time stamp starts over)

03:21

The point about the mixers was well made, emphasizing the nature of data companies versus law enforcement or regulators. They primarily label things based on their definitions. For instance, when it comes to identifying a scam, these companies rely on their own criteria, which is publicly accessible on their websites. This doesn't detract from the authority of nation states, as the purpose is merely to provide labels for further investigation.

03:59

It's assumed that when a blockchain analytics company labels something as a scam, it's the starting point for law enforcement or national authorities to conduct their own investigations. These investigations aim to determine whether the labeled activity aligns with their legal

definitions of a scam. This process doesn't undermine a nation state's authority; rather, it serves as a preliminary step in identifying potential illegal activities.

04:42

Labeling is a necessary part of compliance, especially in distinguishing services that handle large volumes of transactions, which may include illicit funds. It's important to recognize that labeling, such as identifying a mining pool, doesn't imply a negative connotation. It's a statistical measure to understand transaction patterns. The use of terms like "mixer" and "tumbler" may not have been the best choice due to their connotations, but it wasn't the analytics companies that coined these terms.

05:32

The necessity to label certain services, especially when they're used to channel funds from high-risk jurisdictions, is crucial. It's important not to misconstrue the intent behind labeling or to prematurely associate it with illicit activities, except in cases where the label directly implies illegality, such as "scam" or "fraud shop," which are typically recognized as criminal activities across jurisdictions.

06:12

It's essential to understand that these data companies provide initial flags or tips for further investigation. They're not meant to replace comprehensive due diligence. Their alerts serve as starting points, not conclusive evidence that should be taken at face value without further scrutiny.

06:47

The perspective differs significantly between law enforcement and corporate compliance officers. For a compliance officer, a flagged issue requires managing within a corporate context, often with limited investigative capabilities compared to law enforcement. This can trigger complex regulatory assessments without the means to thoroughly investigate the validity of the flag, adding layers of complexity to the situation.

07:33

Acknowledging the pushback on the challenges faced by corporate compliance in dealing with flagged data, it's important to consider the broader implications and the practical limitations of addressing these alerts within a corporate framework.

07:42

There's potential for technological solutions to adapt data taxonomy and labeling to local or regional contexts, akin to customizing XML standards. This flexibility could help reconcile the need for standardization with the necessity for contextual relevance, offering a pathway towards more nuanced and adaptable data handling.

08:37

Inviting diverse perspectives into the conversation can enrich the discussion, especially when considering the customization and adaptation of data standards to fit various contexts. Different viewpoints can lead to more comprehensive solutions that accommodate a range of needs and considerations.

08:51

In the context of decentralized finance (DeFi) and privacy-focused services, there's a growing recognition of the need for accountability, even in privacy-centric projects. Implementing measures like Know Your Customer (KYC) or Know Your Transaction (KYT) can help ensure that these services are not misused for illicit purposes, reflecting a shift towards responsible innovation in the DeFi space.

09:53

The technology available today enables the screening of wallets to exclude those associated with high-risk activities, such as terrorist financing. The emphasis is on fostering an ecosystem where every participant adheres to certain standards of accountability, particularly in the decentralized finance (DeFi) sector, ensuring minimum due diligence is conducted.

10:54

followed by an acknowledgment of the evolving nature of the crypto and DeFi industries. The discussion highlighted the significant advancements in market surveillance within the crypto space, surpassing even traditional finance in some aspects. The responsibility of centralized exchanges in monitoring and regulating activities within their platforms, as well as their role in addressing issues beyond their direct control, was emphasized.

12:38

The existence of tools capable of identifying scams, such as hard-coded rug pulls, was mentioned, underscoring the importance of consumer protection within the industry. The conversation addressed the responsibilities of centralized financial institutions (CeFi) in the crypto space, particularly in terms of compliance and the proactive measures needed to shape effective regulation.

14:05

The formation of the Crypto Market Integrity Coalition was discussed as an example of industry-led initiatives to standardize market integrity and self-regulation. This coalition aims to establish a shared set of standards across the market, demonstrating the industry's commitment to maintaining integrity and addressing challenges.

15:15

The conversation turned to the topic of standardizing a common taxonomy within the industry, questioning the potential role of the running association in leading such an initiative to achieve a widely accepted set of standards.

15:43

It was clarified that the group in discussion is not a traditional industry membership association but rather a community of interest that is proactive and engaged in efforts to set additional standards, including a code of conduct. The discussion touched on the challenges of enforcing standards as a non-government organization.

16:16

The topic of taxonomy and its place on the agenda was brought up, with a clarification that the focus is specifically on market integrity within the crypto space. This includes the introduction of standards and a taxonomy to address market manipulation and abuse, with an emphasis on behaviors unique to the crypto market.

17:10

A query was raised about the strategy for peer-to-peer transactions, specifically how to manage the risk of receiving illicit crypto through indirect transactions. The example given was the potential use of an application by a self-custodial wallet user to provide alerts about the risk associated with a transaction, thus helping to maintain accountability and avoid engaging with illicit crypto.

18:37

The concern was further elaborated with a scenario where an individual might inadvertently receive illicit crypto and face difficulties or consequences when attempting to deposit it into a platform like Coinbase. The question was about how individuals can protect themselves in such situations.

19:11

The discussion explored the practical implications of ensuring the legitimacy of funds in everyday transactions, questioning whether an individual receiving money should be obligated to verify its cleanliness, akin to determining if \$10 handed over for a coffee purchase is not from illicit sources.

19:22

The conversation shifted towards the management of wallets, particularly self-hosted ones, and the comparison of transferring funds to handing over cash in a peer-to-peer context, raising questions about the responsibility to verify the source of funds.

20:03

The discussion highlighted the difference in obligations between regulated institutions like Coinbase and individuals with self-hosted wallets, especially in the context of handling funds from potentially sanctioned or illicit sources.

20:42

The focus turned to the practicalities and limitations of individuals conducting due diligence on transactions, particularly in tracing the origins of funds that might have indirectly come from illicit sources, emphasizing the challenges of ensuring clean transactions in a peer-to-peer setting.

21:38

As the session neared its conclusion, the participants were invited to make final remarks, touching upon the legal implications of unwittingly transacting with funds from sanctioned or illicit sources and the broader question of developing a standardized taxonomy of illicit activities within the industry.

24:05

The importance of information in the hands of blockchain analytics companies, regulators, compliance officers, and law enforcement was emphasized, highlighting the significant role each plays in utilizing the data generated. The creation of information was seen as powerful, but the application of this information was considered even more critical.

24:35

Agreement was expressed on the significance of how the information and taxonomy developed are utilized, underlining the importance of actionable insights derived from data.

24:46

The discussion transitioned to the need for standardization in the industry, acknowledging the challenge posed by the inherent competition and profit motives of companies. The idea was floated that a neutral third party could facilitate standardization, which would be beneficial for providing guidance and ensuring consistency across jurisdictions and industry players.

26:02

It was suggested that widespread adoption of industry standards could drive individual companies to align their products and practices with those standards, leading to a positive ripple effect throughout the ecosystem.

27:25

The conversation highlighted the efforts made in introducing standards and taxonomies over the past years, acknowledging the fragmented nature of these efforts. The potential benefits of consolidating these efforts and the competitive advantage conferred by adherence to established standards were discussed.

28:07

A cautionary perspective was offered on the process of standardization, stressing the importance of inclusivity and considering diverse viewpoints to avoid unintended consequences.

29:34

The session concluded with an invitation to continue the discourse and contribute further to the development of standards and taxonomies, emphasizing the collective responsibility of industry participants to contribute to these efforts.